Security Policies for the
Federal Public Key Infrastructure

Noel A. Nazario
Security Technology Group
National Institute of Standards and Technology

Abstract

This document discusses provisions for the handling of security policies in the proposed Federal Public Key Infrastructure (PKI). Federal PKI policies deal with the generation, deactivation, and dissemination of public key certificates, the integrity of the infrastructure, maintenance of records, identification of certificate holders, and the establishment of trust relationships between Certification Authorities (CAs). The verification of a digital signature is not sufficient indication of the trustworthiness of an electronic message or data file. The verifier needs to factor the trustworthiness of the CAs involved in the certification of the sender. To accomplish this, the verifier needs to examine the certificate policy for those CAs. The Federal PKI Technical Security Policy establishes guidelines for the operation of Federal CAs and the identification of the parties requesting certification. It also defines Policy Approving Authorities (PAA) responsible for assessing the policies and operational practices of all Federal CAs within a domain and assigning them corresponding Federal Assurance Levels. These assurance levels may be used in lieu of a certificate policy when making an on-line determination of the trustworthiness of a certificate.

Key words

Certificate policy, Federal Assurance Levels, PAA, PKI, Policy Approving Authority, public key infrastructure, security policy.

SECURITY POLICIES FOR
THE FEDERAL PUBLIC KEY INFRASTRUCTURE

Noel A. Nazario
NIST North, Room 426
820 West Diamond Avenue
Gaithersburg, MD 20899
NNazario@nist.gov

Introduction and Background

This paper discusses provisions for the handling of security policies in the proposed Federal Public Key Infrastructure (PKI). As shown in Figure 1, the proposed Federal PKI [1] is a public key certificate management system organized administratively as a hierarchy of Certification Authorities (CAs), and their Organizational Registration Authorities (ORAs), that rely on a Directory Service (DS) [2] to disseminate certificates and Certificate Revocation Lists (CRLs). The certificates managed by the PKI [4] support widespread use of digital signatures, and other public key enabled security services, by binding public keys to individuals, roles, or processes and allowing the verification of the authenticity of digital signatures. CAs certify PKI users and each other (cross-certification) to establish trust relationships and define both hierarchical and networked verification paths for user certificates. Hierarchical paths are established by following the certificate path from a root CA to the originator, networked paths are established by finding the appropriate cross-certificates connecting the CAs between the originator and the verifier. Trust is delegated hierarchically and most cross-certificates are required to preserve that delegation. CAs also

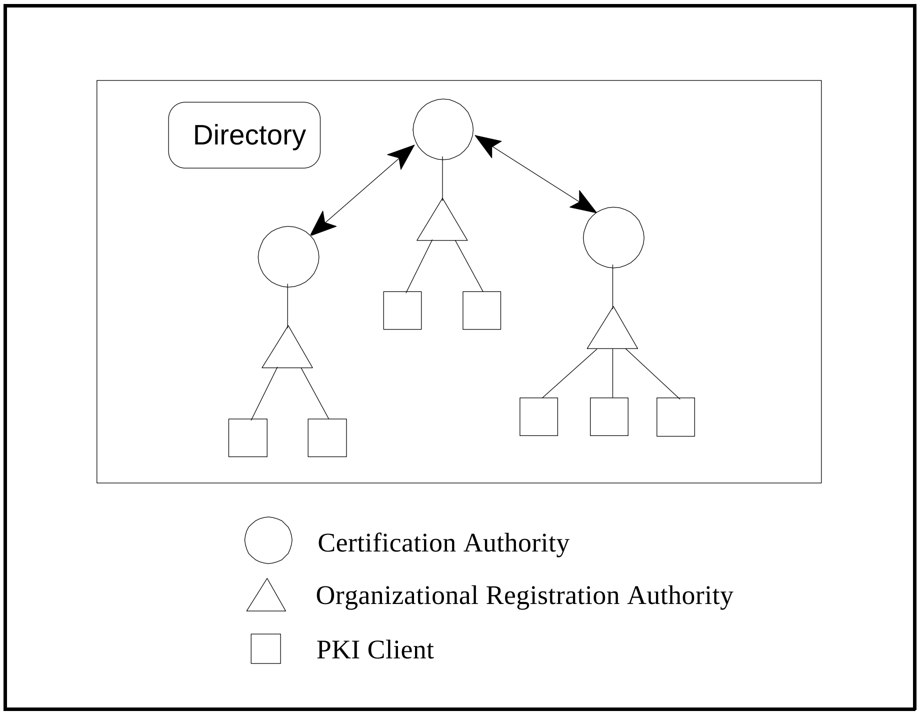

Figure 1 - Main Components of Federal PKI

certify ORAs that verify the identity of users and then vouch them to the CA when requesting initial certification. CA certificates are obtained by one or more agents (authorized operators) of the CA on behalf of the CA, not of the agent(s). ORA certificates are obtained by the agents on their own behalf, i.e., ORA signatures are bound to the agent, not to the ORA.

The Trusted Computer System Evaluation Criteria (TCSEC) [3] defines security policy as a "set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information." Federal PKI policies deal with the generation, revocation, and dissemination of public key certificates, the integrity of the infrastructure, maintenance of records, identification of certificate holders, and the establishment of trust relationships between CAs. The verification of a digital signature is not sufficient indication of the trustworthiness of an electronic message or data file. The verifier needs to factor the trustworthiness of the CAs involved in the certification of the signatory. This is accomplished by examining the certificate policies for those CAs. Federal PKI certificates include a certificate policy field that identifies the security policy under which the certificate was issued. To enable a reasonable judgement on whether to accept a signed document or message, the certificate policy field of the corresponding certificate should point to information about the certificate issuing rules and about the trustworthiness of the CA that granted the certificate. The strictest certificate issuance rules are meaningless if the system that grants the certificate does not verify and protect the integrity of the certificates it generates and does not handle archiving, posting, and revocation of certificates responsibly. The Federal PKI Technical Security Policy (TSP) [5] defines CA Operational Policies and Certificate Issuance Policies that combine into certificate policies that are conveyed by the certificates. CA Operational Policies define the operation of CAs; Certificate Issuance Policies state identification requirements for parties requesting certification.

To ease the assessment of the trustworthiness of a certificate, the TSP defines three Federal Assurance Levels (low, medium, and high). These assurance levels are assigned to each CA by a Policy Approving Authority (PAA) that reviews its policies and practices and determines the highest assurance level that the CA can assign to the certificates it creates. Although they are not actual policies, the identifier for any of these assurance levels can be included in the certificate policies field and used when deciding whether to trust the certificate and the signed document verified with the public key in it. The Federal Assurance Levels are understood by all CAs in the proposed Federal PKI. The PAA performs periodic reviews of the operations of CAs to ensure that an even level of service is maintained throughout the infrastructure.

The policy guidelines discussed in this document apply to all components of the proposed Federal PKI, including CAs, ORAs, directory servers, et cetera. Federal PKI policies are enforced by PAAs.

CA Operational Policy

A CA Operational Policy explicitly defines the operation of a CA. This includes: backup procedures, record archiving procedures, qualifications of operations personnel, functional roles of CA operators, physical protection of the CA, Federal Information Processing Standard (FIPS) 140-1 security level requirements for CA cryptographic modules [6], access controls for CA private keys, et cetera. The CA Operational Policies of CAs in the Federal PKI will be posted in the NIST Computer Security Objects Register (CSOR) [7].

The TSP defines minimum operational requirements for all Federal CAs and additional assurance level-specific requirements for three Federal Assurance Levels; low, medium, and high. The requirements for each level of assurance include the level-specific requirements in addition to those for the level below it.

Minimum Operational Requirements

All CAs within the Federal PKI sign certificates using FIPS-approved signature algorithms. CAs may either generate any parameters that may be required by their signature algorithm or obtain them from the parent CA.
The security policy determines the source of such parameters. The validity period of these parameters is established by the policy of the CA that defines them. The parameters will be maintained for the specified period unless the system is compromised and/or corruption of the locally-maintained certificate-generation data occurs. The parent CA may also request that the parameters used by its subordinates be changed if it is compromised or its database becomes corrupted. If any are required, algorithm parameters will be included in the Subject Public Key Field of the every certificate.

All CAs perform the following functions:

- Generate their own public-private key pairs
- Verify the quality of the public key parameters selected
- Create and deliver subordinate certificates
- Ensure there are no distinguished name collisions within local name space
- When issuing ORA certificates, subordinate CA certificates, and cross-certificates, verify that CAs or ORAs requesting the certificates are in possession of the private keys for all public keys submitted for certification.
- Sign and verify signatures
- Create, maintain, and distribute Certificate Revocation Lists (CRLs)
- Maintain record of certificates issued
- Create and maintain system audit logs
- Archive certificates and CRLs
- Generate or obtain time stamps
- Revoke certificates

CAs need to verify the identity of the originator of certificate requests prior to issuing certificates. Two forms of certification requests will be supported: initial, whereby the identity of the requestor is established in person at request time; and renewal, whereby the established identity of the requestor is verified by the digital signature on the request. Requests for new user certificates (i.e., not renewals) are always generated by an ORA function that vouches for the identity of the user. The ORA function is responsible for providing and verifying all the required personal and affiliation identification information for the type of certificate requested.

Upon receipt of an initial certificate request, CAs: (1)verify the signature of the ORA and that the information on the request is accurate, (2) complete the certificate and sign it with the CA's private key, (3) post the new certificate on a Directory, and (4) return the new certificate along with the CA's own certificate. The certificate may be either returned to the ORA, who then delivers it to the user, or directly to the user. Depending on the CA Operational Policy, the CA may actually return the certificate to both the ORA and the user, thus allowing the ORA to keep record of the certificates issued.

CAs are expected to operate in physically secure environments. The generation of CA private keys, and the hashing/signing of certificates and CRLs occur within cryptographic modules as defined in FIPS 140-1 [6]. In general, the assurance level for an ORA should not be allowed to limit that of the CA, this could be achieved either through security features of the ORA or physical protection and controls. CA and ORA agents are instructed on the operation of their respective systems and provided with reference material on the proper use and safeguard of key material, audit logs, personal information, and archival material. CA and ORA agents are also instructed on the rules and procedures for reporting lost or compromised keys.

Requirements for Low Assurance CAs

Low assurance CAs may only issue certificates that support low-risk applications, such as electronic mail. These CAs may be implemented on systems conforming with FIPS 140-1 Level 2 security requirements and operated by a single CA agent. Keys used for signing certificates are never exported in clear form and should reside in a hardware token under the control of the CA agent.

Requirements for Medium Assurance CAs

CA cryptographic modules must minimally conform to the Level 2 requirements of FIPS 140-1. In addition, medium assurance CAs must provide direct key entry for the input of unprotected key components, separate ports (or pins) for entering plaintext authentication data or keys, and identity-based authentication (all Level 3 requirements). Private keys either remain stored within a cryptographic module or are enciphered using a FIPS-approved algorithm, and cryptographically split, before being output. Security practices such as separation of privilege must be employed.

Requirements for High Assurance CAs

Cryptographic modules for high assurance CAs are implemented in hardware and meet FIPS 140-1 Level 3 requirements.

Certificate Issuance Policies

Certificate issuance policies state the requirements or constraints under which certificates are issued. This includes (1) the personal identification requirements for regular users, subordinate CA agents, and ORA agents being certified, (2) procedures for the generation, safe keeping, revocation, and archiving of key material, and (3) an optional statement of the community for which a CA intends to issue certificates. The TSP specifies issuance policies for CA certificates , ORA agent certificates, and three types of user certificates. Low assurance level user certificates are called L-type certificates, medium assurance user certificates are called M-type certificates, and high assurance level user certificates are called H-type certificates. There are basic similarities between the issuance policies for all these certificate types, the main differences are in the rigor of the identification and authentication requirements, certificate validity periods, key sizes, and number of certificate renewals allowed. The issuance policy details not discussed here are determined by the specific policies of each CA.

For initial certification, CA and ORA agents and users identify themselves in person to the issuing CA. CA and ORA agents identify themselves by presenting their organization's picture id and a letter from a recognized sponsor identifying them as agents. Government users identify themselves by presenting their organization's picture id, other users present any Government issued picture id (e.g., drivers license, passport). Once requesters establish their identities with the issuing CA, or its ORA, they provide a self-signed skeleton certificate containing the public key (i.e., a certificate request). Certificate requests for CA, ORA agent, and H-type certificates must be presented to the ORA on hardware cryptographic tokens, those for other certificate types may be presented on a diskette. The hardware cryptographic tokens used by users requesting certificates for high assurance CAs and H-type user certificates must minimally conform to FIPS 140-1 Level 3. These cryptographic tokens must be unable to export the signature private key.

For every user or agent requesting a certificate of any type, except possibly for L-type user certificates, the CA must receive a request from a recognized user sponsor to issue that certificate. These requests are made through out of bands means and usually consist of a list of names with identification information and the type of certificate requested. ORAs instruct and/or train users, at a level appropriate to the assurance level of their certificates, on the proper use and safeguard of their PKI clients and key material, including rules for reporting lost or compromised keys.

Certificate renewal requires an electronic request signed with both the current, unrevoked, private key and the new signature key. The double signature binds the new key to the existing certificate and allows the parent CA to verify that the requester possesses a valid new key pair. CA policies state how many times certificates of each type may be renewed. Revoked certificates may not be renewed; replacement of revoked certificates must follow the initial certification procedure. The required signature key sizes and their validity periods for each type of certificate are also determined by CA policies.

Federal Assurance Levels

A Federal Assurance Level is an indication of the general level of trust that can be placed on a certificate that will be broadly understood throughout the Federal PKI. The assessment of the trustworthiness of the information in a certificate is made by the PAA upon evaluating the policies and procedures followed by the certifying CA. This effectively maps the actual CA Operational Policy and Issuance Policy followed in generating each certificate onto a Federal Assurance Level. Although Federal Assurance Levels will be conveyed in the certificate policy extension of Federal PKI certificates, they are not actual policies. The three Federal Assurance Levels defined in the TSP (low, medium, high) will be registered by the CSOR under the certificate policies branch. A single Federal Assurance Level will be assigned to every certificate.

Policy Approval Authority (PAA)

A Policy Approving Authority (PAA) is the policy approval and enforcement entity for a specific domain within the Federal PKI. It is responsible for the oversight of the operations of all infrastructure components in its domain. The PAA is directly associated with the root CA for its domain, but it delegates oversight responsibilities to subordinate authorities. The PAA evaluates CA Operational Policies and Certificate Issuance Policies to assess the overall quality of the certificates issued by each CA. This assessment is based on the guidelines outlined in the TSP [5]. The PAA conducts periodic reviews on a periodic basis that it establishes and may revoke the certificates of Federal CAs that fail to implement certificate generation and maintenance procedures in accordance with their own policies. The PAA authorizes Federal PKI CAs to include Federal Assurance Level identifiers in the certificates they issue based on that assessment.

Additional Policy Guidance

Records Keeping

Each CA will log the following certification activities: request to create a certificate, certificates issued, request to revoke a certificate, generation of a CRL, and distribution of a CRL to a Directory. Once a week this information will be stored off-line for archival purposes. All archived information will be maintained in a form that prevents unauthorized modification. Every CA must keep a separate audit log for the monitoring and tracking of security incidents.

Backups

As a minimum all CAs and ORAs within the Federal PKI should conduct daily system backups.

Notification Procedures

Upon occurrence of a system compromise or failure that may affect the integrity of the infrastructure, the CA affected must obtain new certificates, issue the appropriate CRLs, and notify the affected parties of the need to re-authenticate to replace the compromised certificates.

Initialization Procedures

Upon system startup each CA must obtain the certificates it needs from the parent CA and then issue certificates to all its users and subordinate CAs. As new certificates are generated, the Directory server is notified and populated with valid certificates. If the number of users is large, the process may take place in stages. When initialization occurs after a system compromise or failure, an effort will be made to issue notifications to the subscribers if delays are expected to extend beyond 24 hours. Steps must be taken to minimize the possibility of compromise and corruption at all levels of the PKI and to expedite recovery procedures.

Certificate Revocation

CAs will revoke a certificate after validating a request from the certificate holder (a user, CA, or ORA), the ORA that requested the certificate, or the PAA. Common reasons for requesting revocation are: change of the owner's name, separation from the issuing organization, change of the privileges of the user, or failure by a CA to demonstrate compliance with its policies or to implement appropriate operational procedures.

User revocation requests may be directed to either the CA or the ORA. The CAs will accept electronic revocation requests signed with the key being revoked, revocation requests presented in person, or through the telephone. All revocation requests must be verified by the CA prior to taking effect. When the request is made in person, the user needs to provide appropriate identification and the reason for the revocation. Revocation requests over the telephone can only be accepted if a satisfactory personal identification can be made. CAs will issue an electronic notification of the request to the user's superior or agency sponsor. Electronic revocation requests also require verification by the CA.

After processing a request for revocation, the CAs will update and sign the CRL. CAs transmit CRLs to a Directory twice daily, if any new revocations have occurred, or at least once every three days. CRLs are always signed by the issuing CA. Expired certificates are deleted from the CRL.

Certificates are also revoked as part of recovery from compromise or database corruption. If the CA suspects database corruption, in addition to the key compromise, it must revoke all subordinate certificates and electronically notify the subordinates. Old subordinate certificates need not be put on a CRL since the signatures on them will not verify. Subordinates can get the CA's new public key from the Directory. Replacement of revoked certificates is accomplished by following the procedure used for initial registration.

Cross Certification

Cross certification is a mechanism in which two CAs grant each other certificates to signify a trust relationship. This differs from the strict hierarchy model where trust is passed down hierarchically along single certificate paths. The Federal PKI is organized as a hierarchy for administration purposes, but allows the establishment of cross-certificates with some restrictions. The use of cross-certificates allows the establishment of a network of trust relationships among CAs within and outside the Federal hierarchy.

The Federal PKI defines three types of cross-certificates: hierarchical, general, and special. Hierarchical cross-certificates parallel the hierarchical path from the root CA. In the Federal PKI, every CA must trust its parent CA. At certification time every CA cross-certifies its parent to ensure the existence of at least one cross-certificate path to that CA from other Federal CAs. General cross-certificates are intended to simplify certificate paths for efficiency reasons (i.e., to shorten the paths) and may not allow the circumvention of restrictions. Special cross-certificates are intended to establish a relationship between two CAs, not allowed by hierarchical restrictions to certify subordinate CAs. These are called leaf CAs. Using special cross-certificates CAs may circumvent many of the restrictions imposed by their hierarchies. For instance, they could relax the name restrictions imposed by the hierarchical path, or grant each other cross-certificates with an assurance level higher than that of the certificates granted by their respective parent CAs. Only leaf CAs are allowed to establish special cross-certificates to ensure that the circumvention of hierarchically imposed controls is limited to the users of the CAs involved.

Conclusion

The proposed Federal Public Key Infrastructure needs to accommodate the use of dissimilar security policies while providing uniform levels of service and supporting on-line decisions to accept a digital signature. The policies for the Federal PKI deal with the generation, deactivation, and dissemination of public key certificates, the integrity of the infrastructure, maintenance of records, identification of certificate holders, and the establishment of trust relationships between Certification Authorities (CAs). Besides verifying a digital signature, the verifier needs to factor the trustworthiness of the CAs involved in the certification of the sender to determine the trustworthiness of an electronic message or data file. To accomplish this, the verifier needs to examine the certificate policy for those CAs. The Federal PKI Technical Security Policy establishes basic policies for the operation of Federal CAs and the identification of the parties requesting certification. It also creates a management entity that will police the operation of Federal CAs and assess the assurance levels for each CA. These assurance levels can be used in lieu of a certificate policy making an on-line determination of the trustworthiness of a certificate.

References

1. Burr, Nazario, Polk; *A Proposed Federal PKI using X.509 V3 Certificates*, Proceedings from the National Information Systems Security Conference, September 1996.

2. CCITT X.500 Series (1993) | ISO/IEC 9594,1--9, *Information Technology -- Open Systems Interconnection -- The Directory*, 1995.

3. DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

4. Draft Amendments to ITU-T Rec. X.509 | ISO/IEC 9594-8, *Information Technology -- Open Systems Interconnection -- The Directory: Authentication Framework*, August 1995.

5. *Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) - Part B: Technical Security Policy*, Federal PKI Technical Working Group, March 13, 1996.

6. FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, January 1994.

7. NISTIR 5308; N. Nazario; *General Procedures for Registering Computer Security Objects*, December 1993.